Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00056 ISSN 2473-3458

Replication Research of Moody, Siponen, and Pahnila's Unified Model of Information Security Policy Compliance

Kristin Masuch
Georg-August-Universität Göttingen, Göttingen
Kristin.Masuch@uni-goettingen.de

Sebastian Hengstler
Georg-August-Universität Göttingen, Göttingen
s.hengstler@stud.uni-goettingen.de

Simon Trang
Georg-August-Universität Göttingen, Göttingen
strang@uni-goettingen.de

Alfred Benedikt Brendel
Georg-August-Universität Göttingen, Göttingen
abrende1@uni-goettingen.de

Abstract:

Information security compliance behavior research has produced several theoretical models derived from different disciplines to explain or predict violations of information security policies (ISP) or related employee intentions. The application of these theories to ISP violations has led to an increasing number of information security behavioral models. Based on this observation, Moody et al. (2018) reviewed and empirically compared 11 theories that predict information system security behavior using a Finnish sample. Drawing on these findings, they derived and tested a unified model of ISP compliance (UMISPC). This study is a conceptual replication of the refined UMISPC by Moody et al (2018). For the replication, we considered the general tendency to violate policy rather than respondents considering specific behaviors according to the scenario approach that Moody et al. (2018) used to test the refined UMISPC. Further, in contrast to Moody et al. (2018), we tested the refined UMISPC with respondents from Germany. In our data, we found empirical evidence for seven of the eight proposed relationships of the refined UMISPC. Only the relationship between fear and reactance remained insignificant in our estimation. Although more research is necessary to confirm our results, we interpret them as further support for the model's generalizability.

Keywords: Information Security Policy, Compliance, Conceptual Replication

The manuscript was received 07/16/2019 and was with the authors 11 months for 3 revisions.

1 Introduction

As the relevance of information security in private and professional contexts increases, the risk factors for security attacks such as data breaches also increase. One can increasingly see that the human element is a critical factor for the success of information security as unsafe employee behavior causes many violations and technical measures cannot prevent them alone. In order to establish a starting point for socio-technical measures to minimize this risk factor, companies create ISPs that describe compliant and noncompliant employee information security behavior (Angst et al., 2017; Gannon, 2013). One topic related to these endeavors located in information systems (IS) research is the ISP compliance behavior. Unfortunately, research has shown that employees often neglect the appropriate ISP actions prescribed by their respective security policies and, for the most part, tend to behave insecurely, even if they are aware of the guidelines (Cram et al., 2019; Gwebu et al., 2020).

Several studies have analyzed this phenomenon from different angles to explain the aspects of individual security behavior. Various theories from different disciplines, such as criminology and social psychology, have been instantiated and/or modified (e.g., Abraham, 2011; Bulgurcu et al., 2010; D'Arcy and Herath, 2011; Ifinedo, 2012; Willison and Warkentin, 2013). According to Moody et al. (2018), this has led to "a jungle of competing ISP behavior models" that are not easily comparable to one another. For this reason, they reviewed and empirically compared 11 theories that predict compliant ISP behavior. Drawing on these insights, they empirically developed and validated a unified model of ISP compliance (UMISPC).

For the validation of the designed UMISPC, Moody et al. (2018) conducted an online survey and obtained 393 usable responses. Based on the results, they were able to refine their model, called the refined UMISPC, and show that it is valid. The model takes into account the similarities and differences of the combined 11 theories, thus enabling the integration of various important aspects of different ISP compliance behavior models. Further studies with different contextual parameters, such as samples, cross-cultural approaches or different security threats, should be conducted to validate universalized models (Aurigemma and Mattson, 2019). Thus, a replication study is considered necessary to assess whether the UMISPC is stable across cultures, samples, and contexts.

The aim of this replication study was twofold. First, we followed the idea of a conceptual replication as put forth by Dennis and Valacich (2014). The empirically developed scales of the UMISPC are anchored to specific scenario behaviors, whereas we used revised scales that assess one's general tendency to violate ISPs. Second, we validated the UMISPC with German respondents as compared to Moody et al's (2018) study, which used respondents from Finland. Hence, our replication provides a test of the UMISPC's cross-cultural generalizability. In order to generate a broad sample to test the UMISPC, the surveyed German employees include various educational qualifications, as opposed to Moody et al. (2018), who only used graduate students. Altogether, we collected and analyzed a data set of 433 German employees.

The rest of this article is structured as follows. In Section 2, we provide an overview of the development and refinement of the UMISPC. In Section 3, we present our methodology, our data collection process, and our sample's properties. In Section 4, we present our findings and compare them with those of the original study.

2 Research Model

Figure 1 presents the research model, pathways and results of Moody et al.'s (2018) UMISPC validation study, which served as the basis for the development of the refined UMISPC, which was conceptualized in a further step. Table 1 includes the definition of the constructs used to develop the UMISPC.

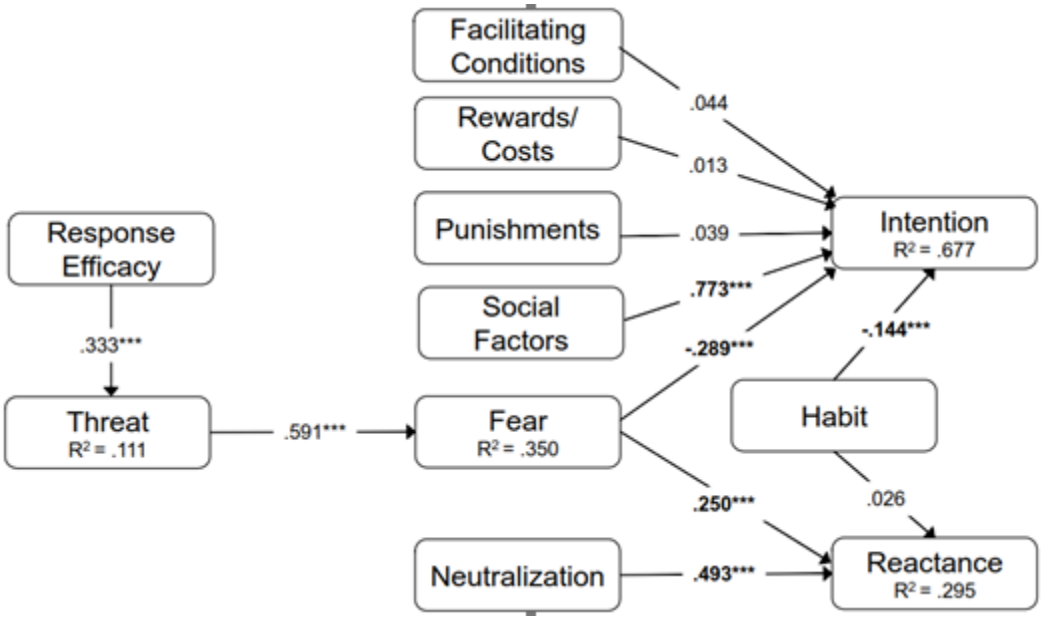

Figure 1. UMISPC Results of the Original Study (Moody et al., 2018).

Table 1. Construct Definitions of the UMISPC (Moody et al., 2018).

Construct	Definition
Response Efficacy	The perceived effectiveness of the behavior in mitigating or avoiding the perceived threat
Threat	Perceived severity and susceptibility to a perceived potential harm
Facilitating Conditions	The potential of the individual to comply without help from other people
Rewards/Costs	Positive reinforcement that is perceived when in compliance with the ISP
Punishments	Negative reinforcement that is perceived to be imposed if found to be noncompliant with the ISP
Social Factors	The summative influence perceived by an individual due to social norms, roles within the group, and the individual's self-concept relevant to the group
Fear	Negative emotional response to stimuli
Neutralization	Rationalized thinking that allows one to justify departure from compliance intentions
Habit	A regular tendency that does not require conscious thought to be compliant with the ISP
Intention	The inclination to engage in a specific behavior
Reactance	Denying that there is an information systems security problem

Moody et al. (2018) were able to provide significant evidence for the intention to comply with ISP and demonstrate reactance. They also found that the constructs of neutralization, fear, habit, and role values

(referred to as social factors in the original model) are significant predictors of intention and reactance. Their results showed that both neutralization and fear significantly predicted reactance. Furthermore, response efficacy could predict the perceived threat, which in turn predicted fear. The protective behavioral intentions for compliance with ISP were explained by the variables of role values, fear, and habits. The punishments, rewards/costs, and facilitation of conditions had no significant impact on intention.

Moody et al.'s (2018) refined UMISPC (Figure 2) only includes constructs and relationships that were found to be significant. In our replication, we examined the refined UMISPC.

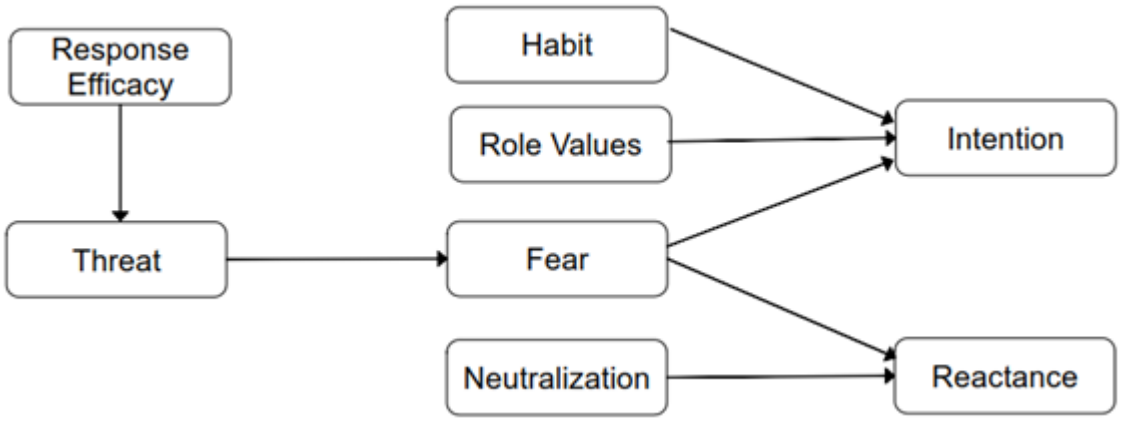

Figure 2. Refined UMISPC of the Original Study (Moody et al., 2018).

3 Method

In this study, we measured the UMISPC items in the context of German employees' ISP compliance behavior. We used the same research questions and hypotheses as to the original study (Dennis and Valacich, 2014). However, we altered the wording of items used to measure the key constructs of the UMISPC in order to generalize each construct's context. In this case, we considered the directions proposed by Moody et al. (2018) to check whether the results in other demographic groups surveyed would lead to different results. Thus, we collected data with items similar to those used by Moody et al. (2018) but in a generalized form, using a survey approach that was not scenario-based in order to avoid a contextual distinction and achieve more general results. A distinction in the modelling of generalizable and context-specific models to explain behavior is controversial in IS research. On the one hand, existing research determines universal relationships that can apply to many information security phenomena that affect employee ISP compliance behavior. Universal constructs and relationships, therefore, constitute the starting points for future research related to many different information security problems. On the other hand, behavior concerning violations of ISPs is often an individual phenomenon, which can vary widely between contexts. Factors such as the company's industry, organizational forms, national culture, or the characteristics of the context of an offence can determine the behavior of an employee in each case. The use of generalized questions aims to measure general behavior for the review of a universal model such as UMISPC. Findings of general behavior about ISP compliance can be used in future research to identify specifics of behavior in different contexts (Aurigemma and Mattson, 2019).

Existing information security behavior research has shown that in some of the models, on which the UMISPC is based, ISP conformity is culturally dependent; hence, there is a need to further test such models for cultural differences (Hovav and D'Arcy, 2012). German nationality was a criterion for participation in our online survey to test the stability of the model and its applicability in a different culture. The participants were recruited through Amazon Mechanical Turk (MTURK) and Clickworker (CW). Participants were remunerated upon completion of the study. We conducted a preselection to ensure that only people who were employed at the time and worked with a computer and whose organizations had ISPs in place would participate. MTURK and CW are reliable sources of high-quality data and have been used in several areas for various research purposes (Lowry et al., 2016; Paolacci and Chandler, 2014).

We conducted a priori sample size calculations using Westland's (2010) formula. It states two lower bounds for sample size in structural equation modelling. The first lower bound referred to the minimum sample size for model identification and the second lower bound referred to the minimum sample size for adequate power to detect an impact. For our calculations, we used the UMISPC as a reference model with eight latent variables and 39 observed variables. Moreover, a statistical power level of 0.9, a probability level of 0.05, and a medium effect size for structural equation modelling of 0.3 were assumed. For the calculations, we used Soper's (2019) a priori sample size for the structural equation models. The minimum sample sizes for model identification and adequate power were 88 and 239, respectively. With 393 participants, Moody et al. (2018) were able to meet both criteria. As we aimed to mimic the original study, we recruited 433 participants for our replication.

To validate our questionnaire, we sent it to five academic experts for review. We then started with 86 participants, obtaining 50 valid and complete questionnaires. As we collected our data from two different sources (i.e. two panel providers), it was necessary to show that the same constructs are measured in both samples. Accordingly, we tested for configural and metric measurement invariance (Steelman et al., 2014). Using the same item configurations, we separately estimated two models. A comparison between the two estimations showed no significant differences in the factor loadings and path coefficients. Moreover, the interpretation of the results was stable in the two groups. We interpreted this as justification for pooling our samples. To conduct a common method bias test, we used the marker variable technique (Lindell and Whitney, 2001) and chose the respondent's outside activities as the theoretically unrelated marker variable (D'Arcy and Lowry, 2019). The highest variance that the marker shared with another construct is less than 0.05. In addition, the path coefficients between the constructs showed no significant size changes (> 0.01). Consequently, we found no evidence of common method bias in our study.

To collect the data from the crowdsourcing platforms mentioned above, we adopted the quality criteria from Lowry et al. (2016). Participants were paid $1.65 for successful and conscientious participation in the study. In order to ensure that the participation criteria of being currently employed, using a computer at work, and working for an organization with an ISP were met, related queries were made before proceeding with the actual questionnaire. If the criteria were not met, the questionnaire was cancelled and considered as unsuccessful. To check whether the questionnaire was filled conscientiously and ensure that questions were not answered randomly, we included questions to which the participant was asked to give a specific answer or solve a math problem. In addition, the relative number of possible answers per participant were compared and revised those who the distribution of the results per answer was higher than 50%. To meet the quality criteria from Lowry et al. (2016), we conducted a technical preselection on the platforms used, to ensure that only participants who were German, and spoke sufficient English to fill the questionnaire and whose acceptance rate of previous participation in other jobs was higher than 90% would participate. Table 2 provides an overview of the samples.

The resulting sample consisted of 767 respondents. According to our selection criteria, 433 responses were classified as valid (validity rate = 57%). The participants mean age was 35-40. The proportion of female subjects was 33%, male subjects accounted for 65%, and 2% opted not to share their gender.

Table 2. Demographics of the Samples.

Variables	Original		Replication
	Study 1	Study 2	
Sample Size	274	393	433
Country	Finland	Finland	Germany
Mean Age	Not Published	Not Published	35-40
Sex (Female/Male/Other)	Not Published	Not Published	33%/65%/2%

Moody et al. (2018) used their first study to test the initially created model and their second study to test the results of their refined model. In our replication study, only one survey was necessary, as we only tested results of the refined UMISPC.

All the participants in the original study had work experience, a master's degree, or a background in education, representing diverse scientific disciplines, such as medicine, natural science, engineering, business, social science, and educational sciences. The authors excluded theology, sports science, and law. Numerical values pertinent to the statistical representation of the demographic criteria, such as age, gender, work experience, and professional background were not provided in the original article. In our replication study, we queried these characteristics, which are presented in Table 3.

Table 3. Characteristics of the Samples.

Sector	Percentage	Job Level	Percentage	Educational Background	Percentage
Manufacturing	12%	Senior Manager	6%	High School or equivalent	14%
Finance	11%	Middle Manager	17%	Two-Year College or equivalent	13%
IT	24%	Technical Staff	16%	Bachelor's Degree or equivalent	37%
Healthcare	9%	Professional Staff	31%	Master's Degree or equivalent	30%
Education	8%	Administrative	13%	Doctoral Degree or equivalent	3%
Retail	4%	Other	17%	Other	3%
Public Administration	9%				
Other	23%				

4 Data Analysis and Results

For the data analysis, we employed partial least squares estimation using SmartPLS 3.0 software. The following subsections present the comparison of our results with those of the original study.

4.1 Measurement of Constructs

Table 4 shows the constructs of Moody et al. (2018) and our items, all of which were reformulated according to the original items. We carefully reformulated most items as statements to adapt them to a research context without an underlying scenario. The items were measured using a 7-point Likert scale from 1 ("disagree") to 7 ("fully agree").

Table 4. Scales and Factor Loadings.

Factor	Items Old	Original Item	Loadings Old	Rephrased	Items Rephrased	Loadings New
Role values	role3	What Mattila did can be justified due to the nature of Mattila's work.	0.784	Not complying with ISP procedures can be justified due to the nature of my work.	SF01	0.534
	moral1	How morally wrong would it be to do what the person did in the scenario?	0.812	Not complying with ISP procedures would be morally wrong.	SF02	0.407
	affect1	What Mattila did is smart.	0.911	Not complying with ISP procedures is smart.	SF03	0.849
	affect4	What Mattila did is pleasant.	0.786	Not complying with ISP procedures is pleasant.	SF04	0.788
	selfcon1	I would feel guilty if I did what Mattila did.	0.889	I would feel guilty if I do not comply with ISP procedures.	SF05	0.369

Table 4. Scales and Factor Loadings.						
	selfcon2	What Mattila did is consistent with my principles.	0.752	Not complying with ISP procedures is consistent with my principles.	SF06	0.816
	selfcon3	It is acceptable to do what Mattila did.	0.833	Not complying with ISP procedures is acceptable.	SF07	0.828
	percbehcont2	If you were Mattila, how much would you feel able to not do as he did?	0.866	I would feel able to not comply with the ISP procedures.	SF08	0.577
Habit	habit1	Not complying with information security procedures saves work time.	0.785	Not complying with information security procedures saves work time.	HAB01	0.739
	habit2	Complying with information security procedures is something I do frequently.	0.800	Complying with information security procedures is something I do frequently.	HAB02	0.840
	habit3	Complying with information security procedures is something I do automatically.	0.762	Complying with information security procedures is something I do automatically.	HAB03	0.863
	habit5	Complying with information security procedures is something I do without having to consciously remember.	0.849	Complying with information security procedures is something I do without having to consciously remember.	HAB04	0.747
	habit7	Complying with information security procedures is something I do without thinking.	0.799	Complying with information security procedures is something I do without thinking.	HAB05	0.855
	habit8	Complying with information security procedures is something that belongs to my (daily, weekly, monthly) routine.	0.783	Complying with information security procedures is something that belongs to my (daily, weekly, monthly) routine.	HAB06	0.749
	habit11	Complying with information security procedures is something I start doing before I realize I'm doing it.	0.862	Complying with information security procedures is something I start doing before I realize I'm doing it.	HAB07	0.592
	habit12	Complying with information security procedures is something that's typically "me."	0.847	Complying with information security procedures is something that's typically "me."	HAB08	0.805

Table 4. Scales and Factor Loadings.						
Neutralization	neutcond3	Complying with information security procedures is something I have been doing for a long time.	0.791	Complying with information security procedures is something I have been doing for a long time.	NEU01	0.878
	neutloyal1	It is not as wrong to violate company information security procedures that are too restrictive.	0.916	It is not as wrong to violate company information security procedures that are too restrictive.	NEU02	0.910
	neutinjury3	It is alright to violate company information security procedures to get a job done.	0.811	It is alright to violate company information security procedures to get a job done.	NEU03	0.896
	vulner1	It is OK to violate company information security procedures if no one gets hurt.	0.884	It is OK to violate company information security procedures if no one gets hurt.	THR01	0.769
	vulner2	I would be subjected to an information security threat if I were to do what Mattila did.	0.894	I would be subjected to an information security threat if I do not comply with the ISP procedures.	THR02	0.822
	vulner3	My organization would be subjected to an information security threat if I were to do what Mattila did.	0.908	My organization would be subjected to an information security threat if I do not comply with ISP procedures.	THR03	0.826
	sever3	An information security problem would occur if I were to do what Mattila did.	0.854	An information security problem would occur if I do not comply with ISP procedures.	THR04	0.797
Fear	fear7	If I were to do what Mattila did, there would be a serious information security problem for my organization.	0.858	If I do not comply with the ISP procedures, there would be a serious information security problem for my organization.	FEAR01	0.878
	fear10	My computer might be compromised if I did what Mattila did.	0.969	If I do not comply with the ISP procedures, my computer might be compromised.	FEAR02	0.848
	fear11	My computer might become unusable if I did what Mattila did.	0.943	If I do not comply with the ISP procedures, my computer might become unusable.	FEAR03	0.702
Response Efficacy	respeff2	My computer might become slower if I did what Mattila did.	0.836	If I do not comply with the ISP procedures, my computer might become slower.	REF02	0.881

Table 4. Scales and Factor Loadings.						
	respeff3	Complying with information security procedures in our organization keeps information security breaches down.	0.861	Complying with information security procedures in our organization keeps information security breaches down.	REF03	0.891
	respeff4	If I were to comply with information security procedures, IS security breaches would be scarce.	0.861	If I were to comply with ISP procedures, IS security breaches would be scarce.	REF04	0.832
Reactance	react3	I need more guidance from my superiors with work-related information security policies.	0.842	I need more guidance from my superiors with work-related information security policies.	REA01	0.949
	react4	I need more guidance from the IT/information security personnel regarding information security issues related to my work.	0.994	I need more guidance from the IT/information security personnel regarding information security issues related to my work.	REA02	0.956
Intention to Comply	NA	What is the chance that you would do what Mattila did in the described scenario?	0.958	I feel that problems resulting from violating ISP procedures are overly exaggerated.	ISPINT01	0.921
	NA	I would act in the same way as Mattila did if I were in the same situation.	0.982	I think that problems resulting from violating ISP procedures are overstated.	ISPINT02	0.906
	NA	/	NA	I intend to carry out my responsibilities prescribed in the ISP procedures of my organization when I use information and technology in the future.	ISPINT03	0.910

4.2 Measurement Validation

We investigated the measurement model in terms of indicator reliability, internal consistency, convergent validity, and discriminant validity. Regarding indicator reliability (Hulland, 1999), we find five items that do not meet the required threshold of 0.7 (see Table 4) and were thus excluded from our model. Afterwards, all indicators had high-standardized loadings on their respective constructs. As a measure of internal consistency, we calculated composite reliabilities (Table 6). All composite reliabilities clearly exceed the threshold of 0.7 (Bagozzi and Yi, 1988). We also confirmed convergent validity, as the average variance extracted (AVE) of each construct was above 0.5 (Bagozzi & Yi, 1988). To assess discriminatory validity (Table 5), we followed Fornell and Larcker's (1981) criterion and compared the square root of the AVEs with the inter-construct correlations. The comparison showed that each construct had a lower correlation value with other constructs than the square root of the AVE (Fornell and Larcker, 1981). Accordingly, discriminant validity was confirmed.

Table 5. Inter-Construct Correlations.

Variable	Intention	Reactance	Fear	Threat	Habit	Neutra-lization	Role value	Response efficacy
Intention	.957							
Reactance	.425	.901						
Fear	-.382	-.304	.921					
Threat	-.438	-.454	.635	.923				
Habit	-.435	-.226	.175	.279	.853			
Neutra-lization	-675	.544	-.294	-.443	-.410	.866		
Role value	.833	.438	-.264	-.393	-.370	.655	.872	
Response efficacy	-.238	-.255	.230	.341	.252	-.223	-.205	.883

Descriptive statistics of the original study. The diagonal represents the square root of the averaged variance extracted (AVE) for the respective construct.

Variable	Intention	Reactance	Fear	Threat	Habit	Neutra-lization	Role value	Response efficacy
Intention	.912							
Reactance	-.392	.953						
Fear	.187	.040	.813					
Threat	.450	-.191	.489	.804				
Habit	.619	-.260	.200	.443	.810			
Neutra-lization	-.506	.608	.002	-.215	-.386	.895		
Role value	.542	-.531	-.004	.206	.401	-.634	.862	
Response efficacy	.295	-.030	.300	.326	.297	-.086	.155	.868

Descriptive statistics of the replication study. The diagonal represents the square root of the averaged variance extracted (AVE) for the respective construct.

Table 6. Descriptive Statistics and Construct Reliability

Variable	Original Study			Replication			
	Mean	Std Dev	CR	Mean	Std Dev	CR	AVE
(1) Intention	-.024	2.984	.9783	5.616	1.179	.9372	.8326
(2) Reactance	-.014	1.306	.9095	3.601	1.431	.9514	.9074
(3) Fear	-.001	1.842	.9351	4.517	1.256	.8528	.6609
(4) Threat	-.009	1.469	.9332	4.548	1.107	.8795	.6461
(6) Habit	.004	.653	.9067	5.161	1.158	.9299	.6555
(7) Neutra-lization	.025	1.836	.8871	3.052	1.459	.9235	.8010
(8) Role value	.007	1.571	.8975	4.959	1.410	.9204	.7432
(11) Response efficacy	-.002	1.249	*	4.587	1.247	.9019	.7541

In our replication of the study, we calculated the mean and standard deviation of the unstandardized variables, which were measured on a scale of 1-7.

* Not reported in the original study.

4.3 Structural Model

We used the PLS method to estimate the refined model. To assess the significance of the paths, we used the bootstrapping resampling method with 3,000 samples. The results and significance are shown in the respective paths in Figure 3. The significant paths were found to be similar to those of Moody et al. (2018). The only non-significant pathway in our estimation that shows significance in the refined UMISPC was the pathway between fear and reactance. In summary, we can conclude that response efficacy (0.325; significant at 0.01) has a significant positive associated with threat. Threat (0.489; significant at 0.01), in turn, was a significant positive predictor on fear. Fear (0.039) had no significant association with other variables. Neutralization (0.608; significant at 0.01) was significant positive associated on reactance. Habit (0.455; significant at 0.01), role values (0.360; significant at 0.01), and fear (0.098; significant at 0.01) were a significant positive predictor of intention. The R^2 of the dependent variable threat was 10.6%, of fear 23.9%, of reactance 37.1%, and of intention 49.5%. Per the original paper, we conclude that the refined UMISPC worked with our sample in all respects except for the path between fear and reactance.

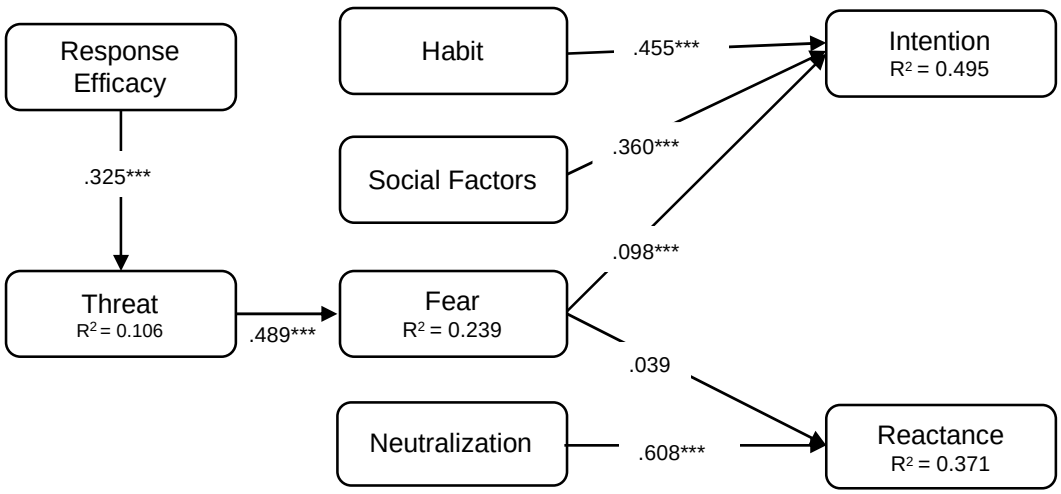

Figure 3. UMISPC Results of the Replication Study.

Table 7. Comparison of the path coefficients and R^2.

Path	**Comparison of Path Coefficients**	
	Original Study	**Replication Study**
Response Efficacy --> Threat	.333***	.325***
Threat --> Fear	.591***	.489***
Habit --> Intention	-.144***	.455***
Social Factors --> Intention	.773***	.360***
Fear --> Intention	-.289***	.098***
Fear --> Reactance	.250***	.039
Neutralization --> Reactance	.493***	.061***
Construct	**Comparison of R^2**	
	Original Study	**Replication Study**
Threat	.111	.106
Fear	.350	.239
Intention	.677	.495
Reactance	.295	.371

*Note: The model of the original study contains further variables (facilitating conditions, rewards/costs, punishment), which were not considered in the measurement of the replication study.

Table 7 shows a comparison between the path coefficients and the R^2 from the structural models of the original and replication study. The comparison revealed both similarities and differences of the relationships between the model's independent and dependent variables. While the influence of response efficacy on threat and of threat on fear are similar in both studies, apparent differences can be observed in other associations. The relationship between social factors on employee's intention was stronger by 0.413 in the original study. The impact of neutralization on reactance was also higher in the replication study (0.4322) than in the original study. The influence of fear on reactance was not very different, although the declared variance in the original study was at a significant level, which was not the case in the replication study. Also, whereas in the original study, habit and fear were positive predictors of intention, they had a negative influence in the replication study.

In closing, with regard to the R^2, it can be stated that in the replications study, these are lower for all constructs except for reactance. Here the R^2 of the replication study is 37.1% and of the original study 29.5%.

5 Discussion

Replication studies are valuable because they enable information security researchers to validate existing models and understand the phenomenon in new contexts (Dennis and Valacich, 2014). This study fulfils the primary objective of a replication study by replicating the refined UMISPC by Moody et al. (2018) in a new context. Furthermore, this work builds on their results by moving away from the original scenarios (USB drive usage, workstation logoff, and password misuse) and applying a generalized, statement-based approach to the description of information security compliance mechanisms in behavioral ISP research. The results of our replication study confirm the stability of some of the model's constructs, extending our knowledge about their stability and applicability in a general ISP behavior context.

Moody et al. (2018) developed a robust model that combines various models from previous behavioral ISP research and tested it in the context of USB drive abuse, password misuse, and failure to log off workstations. Furthermore, they suggested four directions for future research: The first is testing the UMISPC in different contexts to determine its boundaries and identify situations in which the model's components fail to explain the phenomenon analyzed. In our replication, we stepped away from the three contexts initially used, relying on a generic approach to explain the mechanisms considered in the model. Our results show different significances of the constructs, especially regarding fear and habit in association with intention. This supports the view that contextual differences such as cultures, must be taken into account when creating universal models and measuring ISP compliance behavior (Aurigemma and Mattson, 2019; Trang, 2018). We can conclude that the association of the fear and habit constructs with the intention in the German cultural context are different from in the Finnish one. On the other hand, we show that the relationships of other constructs, such as the association of response efficacy with fear and of fear with threat are relatively stable across cultures and a generalized operationalization of the constructs.

The second aim of future research suggested by the authors of the original study is to extend the research stream around the UMISPC by adding additional constructs and moderators in different contexts. We addressed this by using the same model constructs but without adopting a scenario-based approach to collect the data. Instead of the scenarios for measuring intention, we used the constructs proposed by Bulgurcu (2010), which are widely used in the field (Anderson and Agarwal, 2010; Ifinedo, 2012). This helped us determine whether context characteristics rather than various insecure behaviors, such as misuse of passwords, USB drive abuses, or forgetting to log off influence the model's results (Siponen and Vance, 2014). We studied the refined UMISPC model, which was not empirically tested in the original study and was indicated by the authors as a potential object of future research. We found several significances. It was found that response efficacy was a positive predictor of threat. The constructs habit, social factors, and fear were significant positive predictors of the intention to behave compliantly, and neutralization affects reactance in our sample (see Figure 3).

The third suggestion from Moody et al. (2018) is to examine whether certain constructs of the UMISPC may not be relevant in different ISP compliance behavior contexts. Indeed, we found differences between the results of the original study and those of our study. Based on our results and their comparison with those of the original study, the further scope for future research can be identified. First, our study offers an approach without contextual references. As also indicated by Moody et al. (2018), the model should be tested in more contexts in order to determine the usability of its constructs in the various areas of information security.

Second, other demographic differences, such as different national cultures of participants or a comparison on a national, cross-cultural level can also be considered in more detail (Hovav and D'Arcy, 2012).

6 Limitations

There is a notable difference between the data sets being used in the original study and those in our replication study. The original study recruited participants using a database that contained former M.A. students from the universities of the authors which they are currently researching with, whereas this study recruited participants using the crowdsourcing platforms MTURK and CW. Our data set differs in terms of the participants' origin and educational background. Differences in the participants' demographics could not be included in the comparison between the two studies. Moreover, statements about causal relationships presented in this model should be tested in future research on various populations in order to present generally applicable results. As we increased the level of variation in terms of educational background in our sample but did not make direct comparisons to the original study, a distinction and comparison of different educational backgrounds might be interesting. Although it is widely practiced in IS research, collecting empirical data through MTURK is sometimes criticized for carrying a risk in terms of verifying the accuracy of statements or a wide diversity of queried organizations (Lowry et al., 2016). Our replication should be interpreted in light of these limitations. Future replication studies should validate our findings using other panels.

7 Conclusion

This study draws on the findings of Moody et al. (2018) by conducting a conceptual replication of the original research model. We tested the refined UMISPC in a different context, then collected and analyzed 433 responses from German employees. Our measurement models display reliable measurement properties. We provide empirical evidence for seven of the eight proposed relationships of the refined UMISPC. Our results address the scope for future research that were identified in connection with the UMISPC model. Therefore, we used a non-scenario based, contextualized, and generalized approach for the empirical validation of the model, thus examining its applicability from a different perspective. In addition, other items were used to measure intention, which meets the need to use other contexts in the model, according to Moody et al. (2018). As previously discussed, stable relationships but also variations in the results were found. Specifically, these differences should be analyzed by further studies. Furthermore, future research could continue this approach and empirically validate the model from other perspectives. Possible approaches include comparing further cultural differences in the data set using contexts different from those in the original model or our generalized approach and including other demographic variables that have not yet been considered.

References

Abraham, S. (2011). Information security behavior: Factors and research directions. Paper presented at the *17th Americas Conference on Information Systems*, Detroit, MI.

Anderson, C. L.; Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, 34(3), 613-643.

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches, *MIS Quarterly*, 41(3), 893-916.

Aurigemma, S.; Mattson, T. (2019). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems*, 20(12), Article 7.

Bagozzi, R. P., Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74–94.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, 18(2), 151-164.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly* 22(1), vii-xvi.

Cram, W. A.; D'Arcy, J.; Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), 525-554.

Dennis, A. R.; Valacich, J. S. (2014). A replication manifesto. *AIS Transactions on Replication Research*, 1, Article 1, 1-4.

D'Arcy, J., Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658.

D'Arcy, J.; Lowry, P. B. 2019. Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal*, 29(1), 43-69.

Fornell, C., D. F. Larcker (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research* 18(39), 39–50.

Gannon, B. (2013). Outsiders: An exploratory history of IS in corporations. *Journal of Information Technology*, 28(1), 50-62.

Gwebu, K.; Wang, J.; Hu, M. J. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal*, 30(2), 220-269.

Henderson, J. C., & Venkatraman, H. (1999). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, 32(1), 472-484.

Hofstede, G. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations across Nations*. 2d ed. Thousand Oaks, CA: Sage.

Hovav, A.; D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. And South Korea. *Information & Management* 49(2), 99-110.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.

Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information technology adoption across time: A cross-sectional comparison of pre-adoption and post-adoption beliefs. *MIS Quarterly*, 23(2), 183-213.

Lindell, M. K.; Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86(1), 114-121.

Lowry, P. B., D'Arcy, J., Hammer, B., Moody, G. D. (2016): 'Cargo Cult' science in traditional organization and information systems survey research: A case for using nontraditional methods of data collection, including Mechanical Turk and online panels. *Journal of Strategic Information Systems,* 25(3), 232-240.

Melville, N., Kraemer, K., & Gurbaxani, V. (2004). Information technology and organizational performance: An integrative model of IT business value. *MIS Quarterly*, 28(2), 283-322.

Moody, Gregory; Siponen, Mikko; and Pahnila, Seppo. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285-311.

Paolacci, G., Chandler, J. (2014). Inside the Turk: Understanding Mechanical Turk as a participant pool. *Current Directions in Psychological Science*, 23(3), 184-188.

Puhakainen, P., Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757-778.

Ringle, C. M., Sarstedt, M., Straub, D. (2012). Editor's Comments: A Critical Look at the use of PLS-SEM in MIS Quarterly. *MIS Quarterly*, 36(1), iii-xiv.

Siponen, M., Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems*, 23(3), 289-305.

Soper, D.S. (2019). A-priori Sample Size Calculator for Structural Equation Models [Software]. Retrieved from http://www.danielsoper.com/statcalc.

Steelman, Z. R.; Hammer, B. I.; Limayem M. (2014). Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, 38(2), 355-378.

Trang, S. (2018). When does deterrence work? A moderation meta-analysis of employees' information security policy behavior. Paper presented at the *39th International Conference on Information Systems*, San Francisco, CA.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. 2003. User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425-478.

Vinzi, V. E., Trinchera, L., Amato, S. (2006). PLS path modeling: From foundations to recent developments and open issues for model assessment and improvement. In W. W. Chin, V. Esposito Vinzi, J. Henseler and H. Wang (Eds.), *Handbook of PLS and Marketing*. 1. ed., (pp. 47–82). Berlin: Springer Berlin.

Westland, C. J. (2010). Lower bounds on sample size in structural equation modeling. *Electronic Commerce Research and Applications*, 9(6), 476-487.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly* 37(1), 1-20.

About the Authors

Kristin Masuch is a Ph.D. student at Georg-August-University Göttingen, Germany, with a Master's degree in Business Informatics from the same institution in 2019. Her research interests include the field of security crisis response strategies and research on the workplace's information security behavior. Her research focuses mainly on investigating the influencing factors and response strategies after a data breach occurs. In this context, she considers the effects on the customer reaction, but also on the market value of the affected company. She also investigates ways to influence employees' information security behavior to avoid crises such as a data breach. Her work has been presented and published at international conferences, workshops, and journals such as ECIS, the WISP Workshop of ICIS, and the *Pacific Asia Journal of the Association for Information Systems*. In this context, she has also acted as a reviewer on several occasions.

Sebastian Hengstler is a Ph.D. student at Georg-August-University Göttingen, Germany, with a Master's degree in Business Informatics from the same institution in 2019. His research interest is in the field of information security compliance behaviour. His research focuses on the analysis of cultural influences on factors explaining information security compliance behaviour. In this context he is mainly concerned with differences in behaviour based on national culture and the influence of culture on the individual level. His work has been presented and published in conferences such as the American conference on Information Systems. In this context, he has also acted as a reviewer on several occasions.

Simon Trang is an Assistant Professor and holds the Chair of Information Security and Compliance at the Department of Business Administration, University of Goettingen. He received his Ph.D. in management science, specializing in management information systems, from the University of Goettingen. His research interests lie primarily in information security management, strategic IT management, and sustainable IS. His research has been published in outlets such as the *Journal of the Association for Information Systems*, *European Journal of Information Systems, Information Systems Frontiers*, and a number of refereed conference proceedings such as International Conference on Information Systems and European Conference on Information Systems.

Alfred Benedikt Brendel is an Assistant professor ("akademischer Rat") at the University of Goettingen, Germany. Alfred holds a Doctor's degree in management science, specializing in Business Information Systems, from the University of Goettingen. His research focuses on the application of Design Science Research to develop novel and innovative design theories. His main areas of research are digital health, smart mobility, crowdworking, and persuasive system design. His research has been published in the proceedings of leading conferences, such as the International Conference on Information Systems and European Conference on Information Systems, and journals, such as *Transportation Research Part D: Transport and Environment* and *Information Systems Frontiers.*